

REMARKS

The Examiner has rejected claims 1, 21, and 41 under 35 U.S.C. § 101 s being directed to non-statutory subject matter. The Applicant has amended the claims to clarify that the subject matter of the claims is transferring a file for a computer malware scanning software.

The Examiner has rejected Claims 1-10, 12-30, 32-50, 52-60, and 62-63 under 35 U.S.C. 103(a) as being unpatentable over Tso et al. (U.S. Patent No. 6,088,803), in view of Fielding et al. ("Hypertext Transfer Protocol – HTTP/1.1," RFC, June 1999). Applicant respectfully disagrees with such rejection, especially in view of the amendments made hereinabove to the independent claims. Specifically, applicant has amended the independent claims to recite that the randomly accessed portion of the requested file is selected in a random order by the computer malware scanning software from among portions of the file and based on a portion of the file to be scanned by the computer malware scanning software.

With respect to a plurality of the Examiner's rejections, the Examiner has cited pages 82-83 and 85-86 as page identifiers for "Section 14.27: If-Range" and "Section 14.35: Range" of the Fielding reference. Applicant respectfully notes that the above sections relied on by the Examiner are actually found on pages 132-133 and 137-139 of the Fielding reference.

With respect to the independent claims, the Examiner has relied on Col. 3, lines 10-54 and Col. 5, lines 1-43 from the Tso reference to make a prior art showing of applicant's claimed "receiving a request from the computer malware scanning software for data comprising a randomly accessed portion of the requested file" (see the same or similar, but not necessarily identical language in the independent claims).

Applicant respectfully notes that the above excerpts relied on by the Examiner merely teach that "[i]n a typical network transaction, [a] content server... will transmit a requested data object as a series of contiguous portions" (Col. 3, lines 14-16).

Additionally, the above excerpts teach that a “network device... withholds a portion (or a segment of a portion) of the requested file most-recently received from [the] content server... and does not transmit that withheld portion [to the client device] until at least another similarly-sized portion of the requested file is received” (Col. 3, lines 23-28 – emphasis added). Further still, the excerpts teach that a “[v]irus checker... performs virus checking... on the requested file as portions are received from [the] content server” (Col. 3, lines 41-44 – emphasis added). Still yet, applicant respectfully asserts that Col., 5, lines 1-43, as relied on by the Examiner, merely relate to “virus checking” where “checked files and/or results of checks may be advantageously stored in a cache storage” (Col. 5, lines 1-3).

However, merely disclosing a requested data object, as in Tso, fails to meet the applicant’s claimed “receiving a request from the computer malware scanning software for data comprising randomly accessed portion of the requested file selected in a random order by the computer malware scanning software from among portions of the file and based on a portion of the file to be scanned by the computer malware scanning software”, as specifically claimed. In particular, the claims exclude not only error indications and transfer of an entire file, but also exclude transfer of a series of contiguous portions of a file, which is what is disclosed by Tso. Tso does not disclose or suggest selecting portions of a file in a random order based on portions of the file to be scanned by the computer malware scanning software.

Additionally, with respect to the independent claims, the Examiner has relied on Pages 132-133, “Section 14.27: If-Range”; and Pages 137-139, “Section 14.35: Range” from the Fielding reference. The Fielding reference likewise does not disclose or suggest the applicant’s claimed “receiving a request from the computer malware scanning software for data comprising randomly accessed portion of the requested file selected in a random order by the computer malware scanning software from among portions of the file and based on a portion of the file to be scanned by the computer malware scanning software”. Rather, Fielding merely teaches that “[t]he If-Range header allows a client to ‘short-circuit’ the second request...meaning...‘if the entity is unchanged, send me the

part(s) that I am missing; otherwise, send me the entire new entity,” in order to “have an up-to-date copy of the entire entity in its cache” (Page 132, last two paragraphs – emphasis added).

Further, the reference excerpts teach that “[b]yte range specifications in HTTP apply to the sequence of bytes in the entity-body,” and that “[a] byte range operation MAY specify a single range of bytes, or a set of ranges within a single entity” (Page 137, paragraphs 3 and 4). The excerpts also teach that “HTTP retrieval requests... MAY request one or more sub-ranges of the entity, instead of the entire entity, using the Range request header, which applies to the entity returned as the result of the request” (Page 138, last paragraph).

However, sending missing bytes or an entire entity to a client in order to obtain an up-to-date copy of an entire entity, in addition to a byte range operation that specifies ranges of bytes, as in Fielding, does not specifically teach a technique “receiving a request from the computer malware scanning software for data comprising randomly accessed portion of the requested file selected in a random order by the computer malware scanning software from among portions of the file and based on a portion of the file to be scanned by the computer malware scanning software”, as claimed by applicant. Nowhere in the above cited excerpts is there any mention of a selecting portions of a file in a random order based on a portion of the file to be scanned by the computer malware scanning software, as claimed by applicant.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the

prior art and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above. Nevertheless, despite such paramount deficiencies and in the spirit of expediting the prosecution of the present application, applicant has incorporated the subject matter of former Claims 11 et al. and 61 into the independent claims.

Applicant further notes that the prior art is also deficient with respect to the dependent claims. For example, with respect to Claim 8 et al. and Claim 9 et al., the Examiner has relied on Pages 132-133, "Section 14.27: If-Range"; and Pages 137-139, "Section 14.35: Range" from the Fielding reference to make a prior art showing of applicant's claimed "determining that the requested portion of the requested file cannot be transferred; and transferring an entirety of the requested file and supplying the requested data to the computer malware scanning software to fulfill the request for data comprising a portion of the requested file" (see Claim 8 et al.) and applicant's claimed technique "wherein the requested portion of the requested file cannot be transferred because the requested portion of the requested file cannot be randomly accessed" (see Claim 9 et al.).

As mentioned above, applicant again respectfully notes that the above reference excerpts relied on by the Examiner merely teach that "if the entity is unchanged, send me the part(s) that I am missing; otherwise, send me the entire new entity," in order to "have an up-to-date copy of the entire entity in its cache" (Page 132, last two paragraphs – emphasis added). Further, the reference excerpts teach that "[a] byte range operation MAY specify a single range of bytes, or a set of ranges within a single entity" (Page 137, paragraphs 3 and 4). The excerpts also teach that "HTTP retrieval requests... MAY request one or more sub-ranges of the entity, instead of the entire entity, using the Range

request header, which applies to the entity returned as the result of the request” (Page 138, last paragraph).

However, sending the entirety of an entity if the entity is changed, as taught by Fielding, fails to teach “determining that the requested portion of the requested file cannot be transferred” (emphasis added), as claimed by applicant. Additionally, sending missing parts of an entity if the entity is unchanged, in addition to requesting one or more sub-ranges of the entity instead of the entire entity, as also taught in Fielding, does not teach a technique “wherein the requested portion of the requested file cannot be transferred because the requested portion of the requested file cannot be randomly accessed” (emphasis added), as claimed by applicant. More specifically, the above excerpts fail to disclose a situation “wherein... the requested portion of the requested file cannot be randomly accessed” (emphasis added), as claimed by applicant.

Further, with respect to Claims 62 and 63, the Examiner has relied on Col. 3, lines 10-54 and Col. 5, lines 1-43 from the Tso reference to make a prior art showing of applicant’s claimed technique “wherein the data associated with the request from the computer malware scanning software comprises a plurality of randomly accessed portions of the requested file” (see Claim 62, as amended) and “wherein the plurality of randomly accessed portions of the requested file are read in a random order” (see Claim 63, as amended). Applicant respectfully notes that the Examiner cites Claim 64 but relies on the language from Claim 63 in the aforementioned rejection.

Applicant respectfully notes that the above excerpts relied on by the Examiner merely teach that “[i]n a typical network transaction, [a] content server... will transmit a requested data object as a series of contiguous portions” (Col. 3, lines 14-16). Additionally, the above excerpts teach that a “network device... withholds a portion (or a segment of a portion) of the requested file most-recently received from [the] content server... and does not transmit that withheld portion [to the client device] until at least another similarly-sized portion of the requested file is received” (Col. 3, lines 23-28 – emphasis added). Further still, the excerpts teach that a “[v]irus checker... performs

virus checking... on the requested file as portions are received from [the] content server” (Col. 3, lines 41-44). Still yet, applicant respectfully asserts that Col., 5, lines 1-43, as relied on by the Examiner, merely relate to “virus checking” where “checked files and/or results of checks may be advantageously stored in a cache storage” (Col. 5, lines 1-3).

However, merely withholding the most recently received portion of a file from being sent to a client until a similarly-sized portion of the file is received, in addition to performing virus checking on a requested file as portions of the file are received, as in Tso, does not specifically teach a “plurality of randomly accessed portions of the requested file,” much less a technique “wherein the data associated with the request from the computer malware scanning software comprises a plurality of randomly accessed portions of the requested file” (Claim 62, as amended- emphasis added), and a technique “wherein the plurality of randomly accessed portions of the requested file are read in a random order” (Claim 63, as amended - emphasis added), as claimed by applicant.

Further still, the Examiner has rejected Claim 64 under 35 U.S.C. 103(a) as being unpatentable over Tso et al., in view of Fielding et al., and further in view of Ji et al. (U.S. Patent No. 6,728,886). Specifically, the Examiner has relied on Col. 6, line 5 to col. 8, line 10 of the Ji reference to make a prior art showing of applicant’s claimed technique “wherein a system call handler intercepts system level calls made by the computer malware scanning software and simulates system level function calls utilized by the computer malware scanning software to determine whether the file includes the computer malware.”

Applicant respectfully notes that the above reference excerpts relied on by the Examiner merely teach the use of auto-config scripts that “detects the HTTP request (e.g., the request for the search page at Yahoo!) and accesses a virus-scan enabling (VSE) server, which in turn dispatches a set of codes capable of creating a local scan engine and or local proxy server...” (col. 6, lines 25-29) “in order to enable local virus scanning” (Col. 6, lines 55-56). Thus, Ji merely teaches loading and initiating a local virus scanning engine in response to an HTTP request.

However, simply loading and initiating a local virus scanning engine in response to an HTTP request, as disclosed in Ji, fails to teach a technique “wherein a system call handler intercepts system level calls made by the computer malware scanning software and simulates system level function calls utilized by the computer malware scanning software to determine whether the file includes the computer malware” (emphasis added), as claimed by applicant.

Again, since at least the third element of the *prima facie* case of obviousness has not been met, reconsideration of this application and a notice of allowance or a proper prior art showing of all of the claim limitations, in the context of the remaining elements, is respectfully requested.

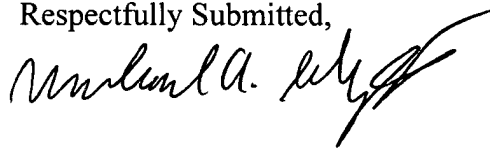
Additional Fees:

The Commissioner is hereby authorized to charge any insufficient fees or credit any overpayment associated with this application to Deposit Account No. 50-4047 (19903.0043).

Conclusion

In view of the foregoing, all of the Examiner's rejections to the claims are believed to be overcome. The Applicants respectfully request reconsideration and issuance of a Notice of Allowance for all the claims remaining in the application. Should the Examiner feel further communication would facilitate prosecution, he is urged to call the undersigned at the phone number provided below.

Respectfully Submitted,



Michael A. Schwartz
Reg. No. 40,161

Dated: March 27, 2008

Bingham McCutchen, LLP
2020 K Street, N.W.
Washington, D.C. 20006
Telephone (202) 373-6000
Facsimile (202) 373-6001